Factorization tests arising from counting modular forms and automorphic representations

Greg Martin
University of British Columbia

joint work with Miao Gu

Number Theory
2018 CMS Summer Meeting
University of New Brunswick
June 3, 2018

these slides can be found on my web page
www.math.ubc.ca/∼gerg/index.shtml?slides

Outline

The quantities we care about

Throughout this talk, k is a positive even integer.

$A(k,N)$ the number of non-isomorphic automorphic representations associated with the space of weight-k cusp forms on $\Gamma_0(N)$ (complicated)

$G(k,N)$ the function from a theorem of Gekeler (simple)

$B(k,N)$ the dimension of the space of weight-k newforms on $\Gamma_0(N)$ (complicated)

$H(k,N)$ a modified version of $G(k,N)$ (simple)

Theme of talk

Whether $A(k,N) = G(k,N)$, and whether $B(k,N) = H(k,N)$, gives us information about the factorization of N.

Some spaces of modular forms and their dimensions

Vector spaces $\mathcal{B}_k(N) \subseteq \mathcal{A}_k(N) \subseteq \mathcal{S}_k(N)$

$\mathcal{B}_k(N)$ the dimension-$B(k,N)$ vector space of weight-k newforms on $\Gamma_0(N)$ (basis: Hecke-eigenform newforms of level N)

$\mathcal{A}_k(N)$ a dimension-$A(k,N)$ vector space whose dimension is the number of automorphic representations (basis: Hecke-eigenform newforms of all levels d dividing N)

$\mathcal{S}_k(N)$ the dimension-$S(k,N)$ vector space of weight-k cusp forms on $\Gamma_0(N)$ (basis: $\tau(\frac{N}{d})$ copies of Hecke-eigenform newforms of all levels d dividing N)

$$S(k,N) = \sum_{d|N} A(k,d) \qquad A(k,N) = \sum_{d|N} B(k,d)$$

$$A(k,N) = \sum_{d|N} \mu\left(\tfrac{N}{d}\right) S(k,d) \qquad B(k,N) = \sum_{d|N} \mu\left(\tfrac{N}{d}\right) A(k,d)$$

Don't read this slide

For any even integer $k \geq 2$ and any integer $N \geq 1$,

$$A(k,N) = \tfrac{k-1}{12} N s_0^*(N) - \tfrac{1}{2}\nu_\infty^*(N) + c_2(k)\nu_2^*(N) + c_3(k)\nu_3^*(N) + \delta\left(\tfrac{k}{2}\right)\delta(N).$$

- $s_0^*(N)$ is multiplicative, with $s_0^*(p) = 1$ and $s_0^*(p^\alpha) = 1 - \frac{1}{p^2}$ for $\alpha \geq 2$.
- $\nu_\infty^*(N)$ is multiplicative, with $\nu_\infty^*(p) = 1$ and $\nu_\infty^*(p^\alpha) = p^{\lfloor \alpha/2 - 1 \rfloor}(p-1)$ for $\alpha \geq 2$.
- $\nu_2^*(N)$ is multiplicative, with
  - $\nu_2^*(2) = 0$, $\nu_2^*(4) = -1$, and $\nu_2^*(2^\alpha) = 0$ for $\alpha \geq 3$;
  - if $p \equiv 1 \pmod 4$ then $\nu_2^*(p) = 1$ and $\nu_2^*(p^\alpha) = 0$ for $\alpha \geq 2$;
  - if $p \equiv 3 \pmod 4$ then $\nu_2^*(p) = -1$ and $\nu_2^*(p^\alpha) = 0$ for $\alpha \geq 2$.
- $\nu_3^*(N)$ is multiplicative, with
  - $\nu_3^*(3) = 0$, $\nu_3^*(9) = -1$, and $\nu_3^*(3^\alpha) = 0$ for $\alpha \geq 3$;
  - if $p \equiv 1 \pmod 3$ then $\nu_3^*(p) = 1$ and $\nu_3^*(p^\alpha) = 0$ for $\alpha \geq 2$;
  - if $p \equiv 2 \pmod 3$ then $\nu_3^*(p) = -1$ and $\nu_3^*(p^\alpha) = 0$ for $\alpha \geq 2$.
- $c_2(k)$ is the function defined by $c_2(k) = \frac{1}{4} + \lfloor \frac{k}{4} \rfloor - \frac{k}{4}$.
- $c_3(k)$ is the function defined by $c_3(k) = \frac{1}{3} + \lfloor \frac{k}{3} \rfloor - \frac{k}{3}$.
- $\delta(m) = \begin{cases} 1, & \text{if } m = 1, \\ 0, & \text{otherwise.} \end{cases}$

Similar formula: $B(k,N) = \tfrac{k-1}{12} N s_0^\#(N) - \tfrac{1}{2}\nu_\infty^\#(N) + c_2(k)\nu_2^\#(N) + c_3(k)\nu_3^\#(N) + \delta\left(\tfrac{k}{2}\right)\mu(N)$.

Calculating these dimensions

- Formula for $S(k,N)$: classical (Riemann–Roch).
- Traditional way to calculate $A(k,N)$ and $B(k,N)$: recursively, starting with values of $S(k,N)$.
- Nowadays: use formulas on previous slide (M., 2005).

Takeaway

$S(k,N)$ (dimension of space of cusp forms), $A(k,N)$ (number of automorphic representations) and $B(k,N)$ (dimension of space of newforms) are linear combinations of explicit multiplicative functions of N, with coefficients depending on k.

All these methods require the factorization of N.

Imagination Station: what would happen if we had fast access to some of the values $A(k,N)$ and $B(k,N)$...?

Gekeler's theorem

Definition (Gekeler's function)

Using the Dirichlet characters χ_{-4} and χ_{-3}, define

$$G(k,N) = \frac{k-1}{12}N - \frac{1}{2} + c_2(k)\chi_{-4}(N) + c_3(k)\chi_{-3}(N).$$

(Note: $c_2(k), \chi_{-4}$ have period 4, and $c_3(k), \chi_{-3}$ have period 3.)

Theorem (Gekeler, 1995)

If N is squarefree, then $A(k,N) = G(k,N)$.

(Then: induction on number of prime factors. Now: evaluate $A(k,N) = \mu(N) * S(k,N)$ immediately.)

Is the converse true?

With one A-value: test for squarefreeness

Theorem 1A (Gu–M., 2018+)

Let $N \geq 2$ be an integer and k a positive even integer.

- *When N is squarefree, or when $k = 2$ and $N = 9$, we have $G(k,N) = A(k,N)$.*
- *When $k = 2$ and $N = 4$, we have $G(k,N) < A(k,N)$.*
- *In all other cases, $G(k,N) > A(k,N)$.*

Imagination Station

If we have an oracle that quickly computes $A(k,N)$ (even for a single k)[a], we have a polynomial-time test for squarefreeness.

[a] or a positive linear combination of several $A(k,N)$, or even a sufficiently tight upper bound for $A(k,N)$

Idea of proof of Theorem 1A

For $N \ge 2$:

$$\begin{aligned} G(k,N) &= \tfrac{k-1}{12}N - \tfrac12 + c_2(k)\chi_{-4}(N) + c_3(k)\chi_{-3}(N) \\ &\ge \tfrac{k-1}{12}N - \tfrac12 - \tfrac14 - \tfrac13 \\ A(k,N) &= \tfrac{k-1}{12}Ns_0^*(N) - \tfrac12\nu_\infty^*(N) + c_2(k)\nu_2^*(N) + c_3(k)\nu_3^*(N) \\ &\le \tfrac{k-1}{12}N\prod_{p^2\mid N}\left(1-\tfrac{1}{p^2}\right) - 0 + \tfrac14 + \tfrac13 \\ &\le \tfrac{k-1}{12}\left(N - \tfrac{N}{p_1^2}\right) + \tfrac{7}{12}. \end{aligned}$$

Theorem (Gu–M., 2018+)

If $d \ge 27$ is an integer such that $d^2 \mid N$, then

$$\sqrt{\frac{(k-1)N}{12\big(G(k,N)-A(k,N)\big)}} \lesssim d \lesssim 2e^\gamma\big(G(k,N)-A(k,N)\big)\log\log N.$$

With two A-values: partial factorization

Another "Imagination Station" result:

Theorem 2A (Gu–M., 2018+)

Let N be a positive integer. Suppose we know two values $A(k_1, N)$ and $A(k_2, N)$ for distinct positive even integers k_1 and k_2. Then we can quickly obtain the complete factorization of the squarefull part of N.

More precisely, we can, in probabilistic polynomial time, calculate distinct primes $p_1, \dots, p_\ell$, integers $e_1, \dots, e_\ell \ge 2$, and a squarefree number E that is relatively prime to $p_1 \cdots p_\ell$, satisfying $N = EL = Ep_1^{e_1} \cdots p_\ell^{e_\ell}$.

Sketch of proof of Theorem 2A

For $N \ge 2$:

$$A(k_1, N) - c_2(k_1)\nu_2^*(N) - c_3(k_1)\nu_3^*(N) = \tfrac{k_1-1}{12} N s_0^*(N) - \tfrac{1}{2}\nu_\infty^*(N)$$
$$A(k_2, N) - c_2(k_2)\nu_2^*(N) - c_3(k_2)\nu_3^*(N) = \tfrac{k_2-1}{12} N s_0^*(N) - \tfrac{1}{2}\nu_\infty^*(N)$$

- By definition, $\nu_2^*(N), \nu_3^*(N) \in \{-1, 0, 1\}$, and we can figure out which from $A(k, N)$; so the left-hand sides are known.
- We can solve these two linear equations for $s_0^*(N)$, $\nu_\infty^*(N)$.
- But the denominator of $s_0^*(N)$ is (morally) the squarefull part L of N, and $N s_0^*(N)$ is a multiple of $\phi(L)$.
- Given L and any multiple of $\phi(L)$, we can probabilistically factor L in polynomial time ("well-known").

From counting automorphic representations $A(k,N)$ to counting newforms $B(k,N)$

Obervation

Since $A(k,N) = 1 * B(k,N)$, we have

$$A(k,N) - B(k,1) = \sum_{\substack{d|N \\ d>1}} B(k,d) \geq B(k,N).$$

Definition

Since we know that $G(k,N) \geq A(k,N)$, define

$$H(k,N) = G(k,N) - B(k,1) = G(k,N) - \left(\tfrac{k-7}{12} + c_2(k) + c_3(k) + \delta\left(\tfrac{k}{2}\right)\right).$$

With this definition, $H(k,N) \geq B(k,N)$, and $H(k,N) > B(k,N)$ as long as N has a proper divisor d with $B(k,d) > 0$.

One B-value: primality test (thanks, referee!)

Theorem 1B (Gu–M., 2018+)

Let $N \geq 2$ be an integer and k a positive even integer.

- *When N is prime, or when $k = 4$ and $N = 6$, or when $k = 2$ and $N = 6, 9, 10, 14, 15, 21, 26, 35, 39, 65,$ or 91, we have $H(k, N) = B(k, N)$.*
- *When $k = 2$ and $N = 4$, we have $H(k, N) < B(k, N)$.*
- *In all other cases, $H(k, N) > B(k, N)$.*

The proof uses the easy (now!) enumeration of all $B(k, N) = 0$.

Imagination Station

If we have an oracle that quickly computes $B(k, N)$ (even for a single k), we have a polynomial-time test for primality.

Two A-values and one B-value: full factorization

Theorem 2A1B (Gu–M., 2018+)

Let N be a positive integer.

Suppose we know two values $A(k_1, N)$ and $A(k_2, N)$ for distinct positive even integers k_1 and k_2, and a value $B(k, N)$ for some positive even integer k.

Then we can calculate the complete factorization of N in probabilistic polynomial time.

Sketch of proof of Theorem 2A1B

From the values $A(k_1, N), A(k_2, N)$, we can write $N = EL$ (with L factored) where E is squarefree and $(E, L) = 1$; say $E > 1$.

From the definition of $B(k, N)$:

$$B(k,N) - c_2(k)\nu_2^{\#}(N) - c_3(k)\nu_3^{\#}(N) - \delta_2(k)\mu(N) = \frac{k-1}{12} N s_0^{\#}(N).$$

Treating the left-hand side as known, we deduce the values $Ns_0^{\#}(N)$ and $Es_0^{\#}(E) = Ns_0^{\#}(N)/Ls_0^{\#}(L)$. But $Es_0^{\#}(E) = \phi(E)$ when E is squarefree; so we can factor E in polynomial time.

Is the left-hand side actually known?

No . . . but the only possible values for $\nu_2^{\#}(N)$, $\nu_3^{\#}(N)$, and $\mu(N)$ are 0 or $\pm 2^m$ for $m \le \omega(N)$. We just try all these (polynomially many) values, and verify the right factorization when we see it.

The end

These slides are available for downloading.

These slides

www.math.ubc.ca/~gerg/index.shtml?slides

(We have a preprint on the arXiv, but we are updating it to include the newer Theorems 1B and 2A1B.)